ITUS MED

January 30, 2015

Karen DeSalvo, MD, MPH, MSc
National Coordinator
Office of National Coordinator for Health IT
Department of Health and Human Services
200 Independence Ave, SW
Washington, DC 20201

Dear Dr. De Salvo:

On behalf of the ITUS Med team, we are pleased for the opportunity to provide commentary on the Federal Health IT Strategic Plan for 2015-2020 as published on www.healthit.gov.

ITUS Med creates a secure private network between hospitals, providers, and patients. This allows for truly secure communication and viewing of sensitive data such as protected health information (PHI).

Current security and encryption methods do not solve the security concerns and breach problems in the market. Browsers and email cannot provide end-to-end encryption. Specifically they do not provide it on the end users device. SSL only provides "in transit" encryption but leaves the data open for attack once the patient opens it via a web browser on their computer or device. Email also does not provide end-to-end encryption and creates an additional risk by exposing users to phishing attacks.

In addition, recent government regulations such as the Final Security Rule governing HIPAA/HITECH extend the requirements for Meaningful Use. This creates much greater urgency to secure this communication and data.

Meaningful Use II requires that hospitals and providers service at least 50% of their patient populations electronically or take payment penalties. Additionally, MUII requires that all PHI be encrypted from end-to-end and institutes significant fines, public disclosure requirements and even jail time for losing PHI. This means patient portals that are delivered through browsers become illegal in 2015 as well as any PHI delivered through email.

ITUS Med's software solves these issues. Our end-to-end encryption is coupled with legal digital signatures giving institutions the added benefit of replacing costly first class mail for bills, lab results, etc.

The ITUS Solution is low cost, easy to deploy and manage, and easy for patients and staff to use through a simple app.

ITUS Med welcomes the opportunity to comment on the following topics related to the sharing and security of protected health information (PHI) and electronic medical records:

1. Goal2: Advance Secure and Interoperable Health Information

ITUS Med is excited the ONC and contributing federal agencies acknowledge the value of enabling individuals, providers, and public health information entities to securely send, receive and use electronic health information. Of particular interest to the ITUS Med team:

The significant progress in digitizing the collection of health information has increased the demand to securely share health information electronically and use it to improve health and health care.

Current standard encryption methods leave end user (patient, other healthcare employees, third party vendors) devices vulnerable outside of the existing internal perimeter security. While the government has already dictated that this information is to be encrypted at rest and in transit from internal networks and on the end user device, the present and future regulatory environment is not well understood and often misinterpreted by existing healthcare IT personnel and executives.

Clear and concise information, education on exactly what is required and explanation of responsibility for the security of healthcare data for both the healthcare organizations and those they service needs to be provided.

2. Objective 2A: Enable individuals, providers, and public health entities to securely send, receive, find, and use electronic health information

ITUS Med strongly supports the initiatives surrounding provider/patient engagement and communication and believe this will foster an overall improvement of healthcare and patient outcomes. Noting the importance of these initiatives:

Since the passage of the HITECH Act, certain types of health information exchange and use among providers have increased; however, gaps and challenges remain for widespread secure and interoperable health information across health care and long-term supports and services providers, settings of care, individuals, health IT platforms, and payers.

Interoperable exchange of health information allows individuals, providers, public health departments, and payers to find, securely exchange, and use vital health information, enhancing care delivery, public health, and research, and empowering individuals to make informed choices regarding their health.

For our nation's healthcare system to achieve interoperability and share medical data internally and with patients, providers, and public health entities, the communications and transmission systems used for sharing regulated information need to consider utilization of advanced secure and encrypted systems which are limited in availability.

Unfortunately, not everyone is going to have the ability to push and pull inbound health data in a

HL7 format and transform that data into something meaningful regarding EHR or other healthcare application. There is a need for systems that can securely transmit health data between interoperable systems, ensure the data is secured end to end as well as provide a receipt of information released and provide mechanisms for tracking information.

Many large healthcare organizations have the necessary resources to secure protected healthcare information internally; however, the sharing of electronic healthcare data in a meaningful way to patients is a weakness even for the largest of our nations healthcare systems. There are ways to make this data available to the patients through web portals, but the security of this data is lacking. If a healthcare provider is truly looking out for the patient's wellbeing, they will ensure that the patient will have the ability to access this data and secure PHI in a robust and meaningful way.

Actual ability to communicate with a patient's healthcare provider is something that is unable to be done currently unless expensive appointments are made. For patients, a simple solution of being able to access their data securely and on their own devices, without having to transform data, is vital and important. ITUS Med offers that exact solution in a way no one else can.

3. Objective 2A: Strategies 4 and 5

Through our development of unique solutions in regard to the secure transmission of protected health information and electronic medical records, ITUS Med encourages a dialogue and exploration in development and deployment of solutions for securing and sharing electronic health information. We are uniquely positioned to respond to strategic needs with respect to:

> *4. Ensure health IT products and services support the privacy, technical, and vocabulary standards necessary for capturing, finding, exchanging, and using standard health information across the health care and long-term services and supports continuum, and with individuals and public health entities*
>
> *5. Encourage electronic information sharing between public and private health providers and payers to promote care continuity*

The best way to promote care continuity, drive improved outcomes, and promote a better overall healthcare system is through the involvement of the patient throughout the entire process. Unfortunately, most of the existing and future methodology for achieving this goal focuses primarily on the providers and payers and forgets the whole reason the system exits, the patient. To truly drive better sharing of data, the patient has to be the primary focus and main communicator to bring together the various healthcare parties that have inherit distrust with each other, providers and payers.

ITUS Med is excited for ONC to focus on this challenge and develops systems to enable the ease of communication to the patient while also ensuring secure environment for the sharing of protected healthcare information and communication between all parties including the payers.

4. Objective 2C: Protect the privacy and security of health information

ITUS Med recognizes the need to protect the privacy and security of health information from a regulatory standpoint and in principle. Our core mission is to develop solutions to satisfy these needs. It is apparent that the ONC is concerned with these matters as follows:

As more health information becomes digitized and shared, it is important that all stakeholders recognize their responsibility in protecting health information. The government will provide oversight and guidance to ensure that stakeholders adhere to laws that protect the privacy and security of health information. Aligning with the HHS' Secretary's Strategic Initiative highlighted in the HHS Strategic Plan 2014-2018 federal actions seek to protect patients' health information, as it is electronically stored and shared and their privacy rights. The federal government is committed to encouraging the development and use of policy and technology to advance patients' rights to access, amend, and make choices for the disclosure of their electronic health information. The federal government also supports the development of policy, standards, and technology to facilitate patients' ability to control the disclosure of specific information that is considered by many to be sensitive in nature (such as information related to substance abuse treatment, reproductive health, mental health, or HIV) in an electronic environment.

The privacy and security of protected health information is a top priority of the federal government, and the government will continue to pursue efforts that ensure confidence and trust for individuals and their families, caregivers, providers, and others.

The required privacy standards are currently being interpreted in many different ways. For most healthcare organizations, they will interpret these requirements in a way that will allow for as small an investment and work to meet these standards as possible. For others, it means transferring the responsibility to their EMR/EHR providers despite it being the organization's responsibility to ensure this data is both protected and secured for all who access it. Smaller organization may struggle to meet the requirement due to a lack of resources, both monetary and technically.

ITUS would encourage meaningful and expanded education about these requirements and the potential penalties and fines that can accompany failure to meet these requirements.

Moreover, ITUS Med strongly supports the strategies regarding Objective 2C:

1. *Support the development and implementation of policies, practices, and education that protect health information from breach, and address cybersecurity risks and developing technologies*

2. *Continue development, administration, and enforcement of federal privacy and security regulations and standards for HIPAA-covered entities and business associates*

3. *Support the development of policies, standards, technology, guidance, and solutions to facilitate individuals' ability to manage, control, and authorize the disclosure of specific electronic health information*

4. *Require and test that certified health IT products incorporate privacy and security*

safeguards

5. *Support, promote, and enhance the establishment of a single health and public health Information Sharing and Analysis Center (ISAC) for bi-directional information sharing about cyber threats and vulnerabilities between the private health care industry and the federal government*

6. *Continue enforcement of applicable federal privacy and security requirements for entities not covered by HIPAA*

With all of the data breaches that are occurring in our nation, we applaud ONC for taking the stance it has in protecting the security of this vital healthcare data, both for the patient and the organization. Unfortunately, the strides being made by healthcare organizations to ensure this protection of the data ceases at their perimeter and does not extend to the end user and consumer of that data. Most patients do not realize the value and danger that their healthcare data being captured by a separate outside party presents. Until healthcare organizations start taking seriously the risk of losing this data, we will continue to see the number of breaches going up, not down.

ITUS Med supports the objectives of the ONC and affiliated organizations in the advancement of sharing healthcare and patient information to facilitate the improvement of the national healthcare system. ITUS Med appreciates an opportunity to submit comments. We hope our comments are helpful and that there will be a meaningful implementation of solutions both public and private to advance our common goals.

We welcome any questions you may have with respect to our comments or requests for additional information. Please feel free to contact us at 801-505-9570 or info@itus-med.com.

Sincerely,

Joe Sowerby
Chief Executive Officer
ITUS Med